IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants:	Cheh Goh and Liqun Chen		
Assignee:	Hewlett-Packard Development Company, L.P.		
Title:	Secure Data Provision Method and Apparatus and Data Recovery Method and System		
Serial No.:	10/825,596	Confirmation No.	7793
Examiner:	Techane Gergiso	Group Art Unit:	2437
Docket No.:	300111166-4	Filing Date:	April 14, 2004

June 2, 2009

Mail Stop APPEAL BRIEF – PATENTS
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Dear Sir:

Appellants submit this Appeal Brief pursuant to the Notice of Appeal filed in this case on April 7, 2009. Appellants submit that this Appeal Brief is being timely filed, but if an extension of time is required for timely filing of this Appeal Brief, an extension of time is hereby requested. Authorization for payment of the fees required for acceptance of this Appeal Brief is provided in an accompanying transmittal letter.

I. REAL PARTY IN INTEREST

The real party in interest is the assignee, Hewlett-Packard Development Company, L.P. Hewlett-Packard Development Company, L.P., is a limited partnership established under the laws of the State of Texas and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

II. RELATED APPEALS AND INTERFERENCES

Based on information and belief, there are no prior or pending appeals, interferences or judicial proceedings known to Appellant, the Appellant's legal representative, or assignee which may be related to, directly affect or be directly affected by or have a bearing on the

Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 23-28 and 43-58 are pending in this case, stand rejected, and are the subject of this appeal. Claims 1-22 and 29-42 have been canceled.

IV. STATUS OF AMENDMENTS

There are no unentered amendments in this case. No amendments were filed subsequent to the Final Rejection dated January 7, 2009.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The claimed subject matter generally relates to secure communication that allows a requesting party clear access to information if a first trusted authority validates that the requesting party is an accredited professional and a second trusted authority validates that an organization that engages the requesting party is accredited. To achieve access, one item must be decrypted using a key that the first trusted authority can generate and another item must be decrypted using a key that the second trusted authority can generate. Fig. 3, which is described in page 11, line 9 to page 15, line 17 of Appellants' specification, illustrates an exemplary implementation of the claimed invention in which the requesting party 20 represents a medical professional such as a doctor or paramedic and the target information is a medical record kept by a storage service 30. The professional can only access a record if the professional is accredited and engaged by an accredited organization. Separate entities 40 and 45 can represent trusted authorities that respectively monitor accreditation of professionals and organizations.

Independent claim 23 recites a secure data-provision method for providing target data (e.g., a patient's medical record PR) from a data provider (e.g., patient record storage service 30 of Fig. 3 and described in page 12, lines 8-12) to a party (e.g., requesting party 20 of Fig. 3 and described at page 12, lines 1-6) purporting to be a specific, professionally-accredited, individual engaged by a specific accredited organization (e.g., medical organization 50 of Fig. 3 described at page 12, lines 26-31), the target data being provided in encrypted form as part of a data set. Requesting party 20, record storage service 30, medical professional trusted authority 40, and medical organization trusted authority 45 include computing entities as

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

described in page 11, lines 18-25 and have distinct capabilities such as described in the above-cited portions of Appellants' specification.

The method of claim 23 includes: encrypting a first item, according to an Identifier-Based Encryption, IBE, scheme, in dependence on encryption parameters comprising a first encryption key string that identifies said specific individual, and public data of a first trusted authority competent in respect of professional accreditations (see page 13, lines 23-25); and encrypting a second item, according to an IBE scheme, in dependence on encryption parameters comprising a second encryption key string that identifies said specific organisation, and public data of a second trusted authority competent in respect of accreditations of organizations (see page 13, lines 25-27); and recovery of the target data in clear requiring decryption of both the first and second items (see page 13, lines 27-30). The method of claim 23 also includes forming the data set using at least the encrypted first and second items, which can be performed using alternative approaches as illustrated in Figs. 4-8. For example, in Fig. 4, the first item is a patient record PR, the encrypted first item is the same as the second item and is the encrypted patient record E<K1,N1;PR>, and the encrypted second item is doubly encrypted patient record E<K2,N2;E<K1,N1;PR>> as described from page 15, line 19 to page 16, line 6.

Independent claim 28 similarly recites a "secure data-provision method for providing target data from a data provider to a party purporting to be a specific, professionally-accredited, individual engaged by a specific accredited organisation, the target data being provided in encrypted form as part of a data set" and can be implemented using the structure of Fig. 3 as described above for claim 23. The method of claim 28 differs from the method of claim 23 in that claim 28 does not expressly require encryption according to an IBE encryption scheme. The method of claim 28 includes: encrypting a first item using both a first encryption key string that identifies said specific individual , and public data of a first trusted authority competent in respect of professional accreditations (see page 13, lines 23-25); and encrypting a second item using both a second encryption key string that identifies said specific organisation, and public data of a second trusted authority competent in respect of accreditations of organisations (see page 13, lines 27-30); and forming said data set using at least the encrypted first and second items (see Figs. 4-8); recovery of the target data in clear requiring decryption of both the first and second items (see page 13, lines 27-30).

Independent claim 43 recites an apparatus (e.g., computing entity 30) for the secure provision of target data (e.g. a patient record PR) to a party (e.g., computing entity 20)

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

purporting to be a specific, professionally-accredited, individual engaged by a specific accredited organisation, the apparatus comprising an encryption subsystem for generating a data set including the target data in encrypted form. In the embodiment of Fig. 3, the encryption subsystem corresponds to crypto module 33 with or without control module 31, which are parts of a computing entity (patient record storage service) 30. Claim 43 recites the encryption subsystem as including means-plus-function elements, and those elements can correspond to computing entities executing instructions that implement the recited functions. The computing entity 30 of Fig. 3 is described in page 11, lines 18-25 and page 12, lines 8-12. Alternative embodiments of the recited functionality are shown in Figs. 4-8. The encryption subsystem includes: first encryption means for encrypting a first item, according to an Identifier-Based Encryption, IBE, scheme, based on encryption parameters comprising a first encryption key string that identifies said specific individual, and public data of a first trusted authority competent in respect of professional accreditations (see page 13, lines 23-25); second encryption means for encrypting a second item, according to an IBE scheme, based on encryption parameters comprising a second encryption key string that identifies said specific organization, and public data of a second trusted authority competent in respect of accreditations of organizations (see page 13, lines 27-30); and means for forming the data set using at least the encrypted first and second items (see Figs. 4-8); the recovery of the target data in clear requiring decryption of both the first and second items (see page 13, lines 27-30).

Independent claim 48 recites a computing entity for recovering target data, which corresponds to computing entity 20 in the embodiment of Fig. 3. (In contrast, claim 43 as described above proves target data as dose computing entity 30 of Fig. 3.) The target data is provided in encrypted form as part of an data set that comprises first and second encrypted items both of which must be decrypted to recover the target data, the first encrypted item (e.g., E<K1,N1;PR> of Fig. 4) being encrypted in dependence on encryption parameters comprising a first encryption key string that identifies a specific individual and first public data, and the second encrypted item (e.g., E<K2,N2;E<K1,N1;PR>> in Fig. 4) being encrypted in dependence on a second encryption key string that identifies a specific organisation and second public data. The entity comprising: first means (e.g., control means 21 and communication module 23 in computing entity 20 of Fig. 3 as described in page 12, lines 1 and 2) for requesting either a first decryption key corresponding to the first encryption key string (see page 14, lines 6-11), or the first item in decrypted form (see page 14, lines 11-13), from a first trusted authority which is competent in respect of the accreditation of

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH (530) 621-4545
FX (530) 621-4543

professionals and holds first private data related to the first public data, the first means being arranged to provide the first encryption key string to the first trusted authority when making its request and being further arranged to authenticate the entity with the first trusted authority and to receive the first decryption key, or the first item, securely from the first trusted authority; second means (e.g., control means 21 and communication module 23) for requesting either a second decryption key corresponding to the second encryption key string, or the second item in decrypted form, from an organization accredited by a second trusted authority (e.g., computing entity 45 of Fig. 3) which holds second private data related to the second public data, the second means being arranged to provide the second encryption key string to the organization (e.g., medical organization 50) when making its request and being further arranged to authenticate the entity (e.g., computing entity 20) with the organisation and receive the second decryption key, or the second item, from the organisation; and third means (e.g., crypto module 22 of Fig. 3) for using the first decryption key, or the first item, provided by the first trusted authority and the second decryption key, or the second item, provided by the organisation, to recover the target data.

Independent claim 54 recites, a computing entity (e.g., computing entity 20 of Fig. 3) for recovering target data provided in encrypted form as part of an data set that comprises first and second encrypted items both of which must be decrypted to recover the target data; the first item being encrypted in dependence on a first encryption key string that identifies a specific individual, and first public data; and the second item being encrypted in dependence on a second encryption key that identifies a specific organisation and said specific individual, and second public data. The data set created using first and second items is described above. The computing entity including: first means (e.g., control and communication modules 21 and/or 23 of Fig. 3) for requesting either a first decryption key corresponding to the first encryption key, or the first item in decrypted form (see page 14, lines 11-13), from a first trusted authority (e.g., computing entity 40) which is competent in respect of the accreditation of professionals and holds first private data related to the first public data, the first means being arranged to provide the first encryption key string, or the first item, to the first trusted authority when making its request (see page 14, lines 6-10); second means (e.g., control and communication modules 21 and/or 23) for requesting either a second decryption key corresponding to the second encryption key string, or the second item in decrypted form, from an organization accredited by a second trusted authority which holds second private data related to the second public data, the second means being arranged to provide the second

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH (530) 621-4545
FX (530) 621-4543

encryption key string to the organisation when making its request (see page 14, lines 15-28); and third means (e.g., crypto module 22) for using the first decryption key, or the first item, provided by the first trusted authority and the second decryption key, or the second item, provided by the organisation, to recover the target data. At least one of the first means and the second means is arranged to authenticate the entity to the first trusted authority or said organisation as the case may be and to receive input therefrom in a secure manner. (See, for example, Fig. 3 and page 16, lines 23-25.)

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following rejection is presented to the Board of Patent Appeals and Interferences for review:

Claims 23-28 and 43-58 are unpatentable under 35 U.S.C. 103(a) over Pat. App. Pub. No. US 2004/0098589 A1 (hereinafter Appenzeller) in view of Pat. App. Pub. No. US 2003/0081785 A1 (hereinafter Boneh).

VII. ARGUMENT

Claims 23-28 and 43-58 are patentable under 35 U.S.C. 103(a) over Appenzeller in view of Boneh.

Independent claim 23 distinguishes over the combination of Appenzeller and Boneh at least by reciting, "encrypting a first item … in dependence on encryption parameters comprising a first encryption key string that identifies said specific individual, and public data of a first trusted authority competent in respect of professional accreditations; and encrypting a second item … in dependence on encryption parameters comprising a second encryption key string that identifies said specific organisation, and public data of a second trusted authority competent in respect of accreditations of organisations; [wherein] recovery of the target data in clear requiring decryption of both the first and second items." The combination of Appenzeller and Boneh fail to disclose or suggest encryption such that recovery of target requires decryption of items encoded using parameters of two different trusted authorities. Appenzeller and Boneh further fails to suggest the encryption parameters of a trusted authority competent in respect of professional accreditations and a trusted authority competent in respect of accreditations of organizations.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

Appenzeller discloses systems and methods for identity-based encryption and discloses ways to reliably provide the public information of different private key generators (PKGs) to parties seeking to encrypt a message for parties associated with other PKGs. In regard to "recovery of the target data in clear requiring decryption of both the first and second items." The Examiner cited paragraphs [0058] and [0068] of Appenzeller. Paragraph [0058] of Appenzeller describes how a random value r may be combined with a receiver's identity Q, and that a message can be encrypted and decrypted based on value rQ. However, this encryption still involves only a single private key generator or trusted authority, and does not suggest that recovery of clear information requires decryption using public information from two different trusted authorities. Paragraph [0068] describes that the receiver's identity Q can be concatenated with a time stamp, so that the key generated is time sensitive and needs to be updated. Again, paragraph [0068] does not disclose or suggest that recovery of clear information requires decryption using public information from two different trusted authorities. Combining Boneh with Appenzeller fails to suggest this feature of claim 23. Accordingly, claim 23 patentably distinguishes over Appenzeller and Boneh.

Claim 23 further distinguishes over the combination of Appenzeller and Boneh because Appenzeller and Boneh fail to suggest using encryption parameters of a trusted authority competent in respect of professional accreditations and a trusted authority competent in respect of accreditations of organizations. Appenzeller does disclose identity-based encryption that may use credential information as part of an identifier value Q, for example, in paragraph [0047] of Appenzeller. Boneh also discloses using credential information as part of an identifier as in paragraph [0053] of Boneh. Assuming for argument that it would be obvious to one of skill in the art to extend this use of credentials to organizations, the combination of Appenzeller and Boneh still fails to indicate a relation or combination of a trusted authority competent in respect of professional accreditations and a trusted authority competent in respect of accreditations of organizations as recited in claim 23.

As indicated in Appellants' specification, access to certain information such as medical records may need to be restricted not only to accredited professions but to accredited professionals who are engaged by accredited organizations. Appellants have discovered a combination of different trusted authorities that allows desired control of sensitive information. The combination of Appenzeller and Boneh fails to disclose co-operative use of trusted authorities (or private key generators) as recited in claim 23.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

For the above reasons, claim 23 is patentable over the combination of Appenzeller and Boneh.

Claims 24-27 depend from claim 23 and are patentable over Appenzeller and Boneh for at least the same reasons that claim 23 is patentable over Appenzeller and Boneh.

Independent claim 28 distinguishes over Appenzeller and Boneh at least by reciting, "encrypting a first item using both a first encryption key string that identifies said specific individual, and public data of a first trusted authority competent in respect of professional accreditations; and encrypting a second item using both a second encryption key string that identifies said specific organisation, and public data of a second trusted authority competent in respect of accreditations of organisations; … [wherein] recovery of the target data in clear requiring decryption of both the first and second items." For the same reasons as noted above with reference to claim 23, the combination of Appenzeller and Boneh fails to disclose or suggest encryption such that recovery of target requires decryption of items encoded using parameters of two different trusted authorities and fails to suggest use of encryption parameters of a trusted authority competent in respect of professional accreditations and a trusted authority competent in respect of accreditations of organizations as in claim 28. Accordingly, claim 28 is patentable over Appenzeller and Boneh.

Independent claim 43 distinguishes over Appenzeller and Boneh at least by reciting, "first encryption means for encrypting a first item … based on encryption parameters comprising a first encryption key string that identifies said specific individual, and public data of a first trusted authority competent in respect of professional accreditations; second encryption means for encrypting a second item … based on encryption parameters comprising a second encryption key string that identifies said specific organisation, and public data of a second trusted authority competent in respect of accreditations of organisations; … [wherein] the recovery of the target data in clear requiring decryption of both the first and second items." The reasons for patentability of process claim 23 again apply to the apparatus claim 43, and claim 43 is patentable over Appenzeller and Boneh.

Claims 44-47 depend from claim 43 and are patentable over Appenzeller and Boneh for at least the same reasons that claim 43 is patentable over Appenzeller and Boneh.

Independent claim 48 distinguishes over Appenzeller and Boneh at least by reciting, "A computing entity for recovering target data …; the entity comprising: first means for requesting either a first decryption key corresponding to the first encryption key string, or the first item in decrypted form, from a first trusted authority which is competent in respect of the

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

accreditation of professionals ..., the first means being arranged to provide the first encryption key string to the first trusted authority when making its request and being further arranged to authenticate the entity with the first trusted authority and to receive the first decryption key, or the first item, securely from the first trusted authority; second means for requesting either a second decryption key corresponding to the second encryption key string, or the second item in decrypted form, from an organization accredited by a second trusted authority ..., the second means being arranged to provide the second encryption key string to the organisation when making its request and being further arranged to authenticate the entity with the organisation and receive the second decryption key, or the second item, from the organisation." The combination of Appenzeller and Boneh fails to disclose or suggest a computing entity with means to provide first and second decryption key strings to a first trusted authority that accredits professionals and an organization accredited by a second trusted authority. More particularly, as noted above, Appenzeller and Boneh generally fail to describe any relationships or co-operation of trusted authorities that monitor accreditation of professionals and organization and specifically fail to disclose arrangements recited in claim 48. Accordingly, claim 48 is patentable over the combination of Appenzeller and Boneh.

Claims 49-53 depend from claim 48 and are patentable over Appenzeller and Boneh for at least the same reasons that claim 48 is patentable over Appenzeller and Boneh.

Independent claim 54 distinguishes over the combination of Appenzeller and Boneh at least by reciting, "A computing entity for recovering target data provided in encrypted form ...; the entity comprising: first means for requesting either a first decryption key corresponding to the first encryption key, or the first item in decrypted form, from a first trusted authority which is competent in respect of the accreditation of professionals and holds first private data related to the first public data, the first means being arranged to provide the first encryption key string, or the first item, to the first trusted authority when making its request; second means for requesting either a second decryption key corresponding to the second encryption key string, or the second item in decrypted form, from an organization accredited by a second trusted authority which holds second private data related to the second public data, the second means being arranged to provide the second encryption key string to the organisation when making its request." As noted above, Appenzeller and Boneh generally fail to describe any relationships or co-operation of trusted authorities that monitor accreditation of professionals and organization and specifically fail to disclose arrangements recited in claim 54. Accordingly, claim 54 is patentable over the combination of Appenzeller

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH (530) 621-4545
FX (530) 621-4543

and Bonch.

Claims 55-58 depend from claim 54 and are patentable over Appenzeller and Bonch for at least the same reasons that claim 54 is patentable over Appenzeller and Bonch.

For the above reasons, Appellants respectfully submit that pending Claims 23-28 and 43-58 are allowable. Accordingly, Appellants submit the present rejection is unfounded and request that the rejection of claims 23-28 and 43-58 be reversed.

Please contact the undersigned attorney at (530) 621-4545 if there are any questions concerning this Appeal Brief or the application generally.

Respectfully submitted,

/David Millers 37396/

David Millers
Reg. No. 37,396

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH (530) 621-4545
FX (530) 621-4543

VIII. CLAIMS APPENDIX

Claims 23-28 and 43-58, which are the claims involved in this appeal, are copied below.

Claims 1-22 (Cancelled)

23. A secure data-provision method for providing target data from a data provider to a party purporting to be a specific, professionally-accredited, individual engaged by a specific accredited organisation, the target data being provided in encrypted form as part of a data set; the method comprising:

encrypting a first item, according to an Identifier-Based Encryption, IBE, scheme, in dependence on encryption parameters comprising a first encryption key string that identifies said specific individual, and public data of a first trusted authority competent in respect of professional accreditations; and

encrypting a second item, according to an IBE scheme, in dependence on encryption parameters comprising a second encryption key string that identifies said specific organisation, and public data of a second trusted authority competent in respect of accreditations of organisations; and

forming said data set using at least the encrypted first and second items;

recovery of the target data in clear requiring decryption of both the first and second items.

24. A method according to claim 23, wherein the first item comprises the target data, and the second item comprises the encrypted first item.

25. A method according to claim 23, wherein the first item comprises the target data, and the second item comprises a nonce; the first encryption key string comprising, in combination, an identifier of said specific individual and said nonce.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

26. A method according to claim 23, wherein the first item comprises first data, and the second item comprises second data; the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data.

27. A method according to claim 23, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key.

28. A secure data-provision method for providing target data from a data provider to a party purporting to be a specific, professionally-accredited, individual engaged by a specific accredited organisation, the target data being provided in encrypted form as part of a data set, the method comprising:

encrypting a first item using both a first encryption key string that identifies said specific individual, and public data of a first trusted authority competent in respect of professional accreditations; and

encrypting a second item using both a second encryption key string that identifies said specific organisation, and public data of a second trusted authority competent in respect of accreditations of organisations; and

forming said data set using at least the encrypted first and second items;

recovery of the target data in clear requiring decryption of both the first and second items.

Claims 29-42 (Cancelled)

43. Apparatus for the secure provision of target data to a party purporting to be a specific, professionally-accredited, individual engaged by a specific accredited organisation, the apparatus comprising an encryption subsystem for generating a data set including the target data in encrypted form, the encryption subsystem comprising:

first encryption means for encrypting a first item, according to an Identifier-Based Encryption, IBE, scheme, based on encryption parameters comprising a first encryption key string that identifies said specific individual, and public data of a first trusted authority competent in respect of professional accreditations;

second encryption means for encrypting a second item, according to an IBE scheme, based on encryption parameters comprising a second encryption key string that identifies said

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH (530) 621-4545
FX (530) 621-4543

specific organisation, and public data of a second trusted authority competent in respect of accreditations of organisations; and

means for forming the data set using at least the encrypted first and second items; the recovery of the target data in clear requiring decryption of both the first and second items.

44. Apparatus according to claim 43, wherein the first item comprises the target data, and the second item comprises the encrypted first item.

45. Apparatus according to claim 43, wherein the first item comprises the target data, and the second item comprises a nonce; the first encryption key string comprising, in combination, an identifier of said specific individual and said nonce.

46. Apparatus according to claim 43, wherein the first item comprises first data, and the second item comprises second data; the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data.

47. Apparatus according to claim 43, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key.

48. A computing entity for recovering target data provided in encrypted form as part of an data set that comprises first and second encrypted items both of which must be decrypted to recover the target data, the first item being encrypted in dependence on encryption parameters comprising a first encryption key string that identifies a specific individual and first public data, and the second item being encrypted in dependence on a second encryption key string that identifies a specific organisation and second public data; the entity comprising:

first means for requesting either a first decryption key corresponding to the first encryption key string, or the first item in decrypted form, from a first trusted authority which is competent in respect of the accreditation of professionals and holds first private data related to the first public data, the first means being arranged to provide the first encryption key string to the first trusted authority when making its request and being further arranged to

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

authenticate the entity with the first trusted authority and to receive the first decryption key, or the first item, securely from the first trusted authority;

second means for requesting either a second decryption key corresponding to the second encryption key string, or the second item in decrypted form, from an organization accredited by a second trusted authority which holds second private data related to the second public data, the second means being arranged to provide the second encryption key string to the organisation when making its request and being further arranged to authenticate the entity with the organisation and receive the second decryption key, or the second item, from the organisation;

third means for using the first decryption key, or the first item, provided by the first trusted authority and the second decryption key, or the second item, provided by the organisation, to recover the target data.

49. A computing entity according to claim 48, wherein the second means is arranged to receive the second decryption key, or the second item, securely from the organisation.

50. A computing entity according to claim 48, wherein the first item comprises the target data, and the second item comprises the encrypted first item; the third means being arranged to: recover the second item, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation, and subject the second item to decryption, using the first decryption key obtained from the first trusted authority, to recover the target data.

51. A computing entity according to claim 48, wherein the first item comprises the target data, the second item comprises a nonce, and the first encryption key string comprises, in combination, an identifier of said specific individual and said nonce; the third means being arranged to: recover the second item, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation, combine the nonce that formed the second item with the identifier of said specific individual in order to form the first encryption key string to be provided by the first means to the first trusted authority, and use the first decryption key obtained from the first trusted authority to decrypt the first item and thereby recover the target data.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

52. A computing entity according to claim 48, wherein the first item comprises first data and the second item comprises second data, the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data; the third means being arranged to recover the first data, if not provided to the first means by the first trusted authority, by using the first decryption key obtained from the first trusted authority, recover the second data, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation, use the first data and the second data to form said symmetric key, and use the symmetric key to decrypt the target data.

53. A computing entity according to claim 48, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key; the third means being arranged to: recover the first item, if not provided to the first means by the first trusted authority, by using the first decryption key obtained from the first trusted authority, recover the second item, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation, use the second symmetric key that formed the second item to decrypt the encrypted first symmetric key that formed the first item, and use the first symmetric key to decrypt the encrypted target data.

54. A computing entity for recovering target data provided in encrypted form as part of an data set that comprises first and second encrypted items both of which must be decrypted to recover the target data; the first item being encrypted in dependence on a first encryption key string that identifies a specific individual, and first public data; and the second item being encrypted in dependence on a second encryption key that identifies a specific organisation and said specific individual, and second public data; the entity comprising:

first means for requesting either a first decryption key corresponding to the first encryption key, or the first item in decrypted form, from a first trusted authority which is competent in respect of the accreditation of professionals and holds first private data related to the first public data, the first means being arranged to provide the first encryption key string, or the first item, to the first trusted authority when making its request;

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH (530) 621-4545
FX (530) 621-4543

second means for requesting either a second decryption key corresponding to the second encryption key string, or the second item in decrypted form, from an organization accredited by a second trusted authority which holds second private data related to the second public data, the second means being arranged to provide the second encryption key string to the organisation when making its request; and

third means for using the first decryption key, or the first item, provided by the first trusted authority and the second decryption key, or the second item, provided by the organisation, to recover the target data;

at least one of the first means and the second means being arranged to authenticate the entity to the first trusted authority or said organisation as the case may be and to receive input therefrom in a secure manner.

55. A computing entity according to claim 54, wherein the first item comprises the target data, and the second item comprises the encrypted first item; the third means being arranged to: recover the second item, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation, and subject the second item to decryption, using the first decryption key obtained from the first trusted authority, to recover the target data.

56. A computing entity according to claim 54, wherein the first item comprises the target data, the second item comprises a nonce, and the first encryption key string comprises, in combination, an identifier of said specific individual and said nonce; the third means being arranged to: recover the second item, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation, combine the nonce that formed the second item with the identifier of said specific individual in order to form the first encryption key string to be provided by the first means to the first trusted authority, and use the first decryption key obtained from the first trusted authority to decrypt the first item and thereby recover the target data.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

57. A computing entity according to claim 54, wherein the first item comprises first data and the second item comprises second data, the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data; the third means being arranged to recover the first data, if not provided to the first means

by the first trusted authority, by using the first decryption key obtained from the first trusted authority, recover the second data, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation, use the first data and the second data to form said symmetric key, and use the symmetric key to decrypt the target data.

58. A computing entity according to claim 54, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key; the third means being arranged to: recover the first item, if not provided to the first means by the first trusted authority, by using the first decryption key obtained from the first trusted authority, recover the second item, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation, use the second symmetric key that formed the second item to decrypt the encrypted first symmetric key that formed the first item, and use the first symmetric key to decrypt the encrypted target data.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH (530) 621-4545
FX (530) 621-4543

IX. EVIDENCE APPENDIX

There is no evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 or any other evidence entered by the examiner that Appellant is relying upon in this appeal.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

X. RELATED PROCEEDINGS APPENDIX

No decisions rendered by a court or the Board of Patent Appeals and Interferences are being submitted.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543